The Dialogue™
INFORM ENGAGE IDEATE

THE PAYMENT AGGREGATORS AND PAYMENT GATEWAYS (PAPG) GUIDELINES

VIRTUAL STAKEHOLDER DISCUSSION

MARCH 30, 2021

The Dialogue™
INFORM ENGAGE IDEATE

The Payment Aggregators and Payment Gateways (PAPG) Guidelines

Virtual Stakeholder Discussion

March 30, 2021

INTRODUCTION

The Dialogue, a New Delhi based Think-Tank, held a virtual stakeholder consultation on 'the PAPG Guidelines' on March 30, 2020. We hosted the following panellists:

- Dr. Aruna Sharma, RBI Digitisation Committee Member
- Mr Ram Rastogi, Digital Payments Expert
- Mr Avimukt Dar, Co-founder IndusLaw

The Reserve Bank of India ('RBI'), in March 2020, released guidelines addressing concerns around the manner in which payment aggregators and payment gateways ('PAPG') collect and store merchant data during the onboarding process. The PAPG guidelines, in Rule 7.4, prohibit merchant websites from storing card-on-file and related data. Compliance with the aforementioned provision will be challenging and has the potential for business disruption. The driving reasons behind the same are the data security and privacy concerns raised from such a mechanism. This point of view has been reinforced by their criticism of security standards such as PCI-DSS and PA-DSS which they feel are not robust enough, and the implementation of these standards has not stopped data breaches of card data in the past. The RBI, in August, relaxed a few of the Additional Factor of Authentication ('AFA') requirements. However, it's still important to analyse if these decisions are optimal for the long-term health of the financial regulatory frameworks in this country.

The objectives behind the discussion were that of dissecting the 'PAPG Guidelines', examining the primary concerns raised by various stakeholders and analysing the efficacy of the revised e-mandate guidelines. The panellists agreed that before drafting guidelines within this space in particular, it's important to consult industry experts and key market players. Their familiarity with the concerns faced not only by consumers but other PA/PG, will allow for greater ease of compliance and will boost the country's digitization efforts.

The discussion raised some extremely pertinent questions around the following themes:

1. Data Protection and Other Consumer Interests

Dr. Sharma pointed out that the end-user will be severely affected by an increased cost of service. Issues of ease will unfold as factors like digital literacy and age will affect one's ability to utilise digital payment services. According to Dr. Sharma, the COVID-19 pandemic has led to an 80-90% jump in the value of UPI Payments. People have grown accustomed to the use of digital payments and associated services, such as repeat payments. Therefore, the hasty implementation of the regulation is likely to disrupt digital services in the short term, and force consumers to begin using cash-based payment methods once again. Such policy measures will negatively affect India's digital India mission.

In addition to the challenges mentioned above, consumers will have to comply with paper-based Know Your Customer (KYC) requirements repeatedly. While this not only increases one's inconvenience, it also poses various privacy-based concerns. The panel unanimously stated that the absence of a data protection law and subsequently, a data protection authority, is posing several challenges within this sector. There are several tussles between different entities, such as those interested in consumer affairs and the RBI, among other concerns being raised such as those relating to the lack of accountability. The primary reason for the same is because there is a regulatory lacuna. The lack of a data protection law allows the regulator to be further absolved from all accountability.

Mr. Avimukt Dar also pointed out that there are several issues with allowing financial regulators to take up the role of data protection. He pointed out that, similar to the practice in the European Union, financial regulators must simply lay down baseline compliance guidelines like Payment Card Industry Data Security Standard ('PCI DSS'). Similarly, Dr. Sharma emphasised the need to have a single authority dealing with data security and privacy. India, as she pointed out, has always done well with the detection of cybersecurity threats or data breaches. The problem, therefore, lies in the reaction time (this extends to banks and fintechs alike). She concluded that while data privacy and security can have two separate policies, it's important to have an interdisciplinary regulator in place.

2. Harmonised Regulation

Dr. Sharma emphasised the need for harmonious regulation within this sector. She pointed out the various policies under this umbrella--the new Foreign Trade Policy (FTP), the new IT Rules, 2021, the various offences provided for in the Indian Penal Code, 1860, and the RBI Regulations etc. The

future of banking, as predicted by her, is not in the brick-and-mortar format. In order to support the future vision of banking, it's important to harmonise various policy measures relating to increased access to internet, internet speeds, data protection etc. A holistic approach is key.

The sheer number of regulations within this sphere point to the urgent need for increased harmony. The European Union, for example, has a Payment Services (PSD 1)- Directive 2007/64/EC which regulates all fintech and other players that handle payments. As pointed out by Mr. Dar, interoperability of data is essential, and a harmonious regulation regime is a step closer to that goal. Mr. Rastogi pointed out the need for a 'single control point' in order to ensure compliance while protecting the interests of the end users and related parties.

3. Embracing New Technology

The panellists agreed that in order to have an effective e-mandate, consultation is key. Mr. Ram Rastogi pointed out that 84% of UPI transactions are facilitated by Google Pay, PhonePe and Amazon. BHIM only constitutes around 2% of these transactions. Therefore, it's important to consult these key market players prior to drafting a policy.

In addition to the need for consultation, Dr. Sharma observed that the regulations were being adopted as a "knee jerk reaction". She stated that the date of implementation of the guidelines (April 1, 2021) must be pushed by a few months in order to ensure that banks and other entities will be able to ensure a smooth transition between systems.

Mr. Rastogi pointed out the need to regulate fintech in a manner that embraces such technology. Mr. Dar compared the adoption of fintech on a global scale to that of e-mails. He stated that the way worldwide fintech is meant to disrupt the banking system, e-mails disrupted letters and telegrams.

In addition to the procedural fallacies pointed out by the panellists, Dr. Sharma also questioned the security and privacy concerns cited by the RBI. She stated that with measures such as One-Time-Password (OTP) and CVV, there is adequate protection. Additionally, Mr. Rastogi drew the panel's attention to an IBM study which stated that of these cybersecurity concerns, most of the "attacks" happen in Japan, while only 8% happen in India. Therefore, the situation is not as grave as it seems.

In order to fully embrace new technology within the financial sector, banks must either turn completely digital , create a digital bank within their bank (similar to State Bank of India) or collaborate with fintech companies. Mr. Dar pointed out that the State is unsure of who poses a threat and where the threat is coming from. The current approach attempts to limit people's rights in order to minimise participation. The assumption here is that data safety can be ensured with limited participation within this space. However, the dangers of such a policy are already being felt

with "cryptocurrencies", where there are transactions happening on a global scale that India is not a part of.

ACTION POINTS AND WAY FORWARD

Based on the insightful discussion from the panelists, it is evident that:

1. In order to ensure ease of compliance and not increase service costs for users, it's important to create a **harmonious regime and increase interoperability.** The first step towards achieving this is to address and amend the discrepancies in applying different compliance requirements to entities offering similar services.
2. An essential step in protecting consumer interests is the creation of a **Data Protection Authority** under a robust data protection framework. This will allow for increased accountability and thereby increase public trust.
3. **Allowing industry players time to implement** the scheme of tokenisation among other measures is essential. **Conducting more consultations** that allow for the harmonisation of needs will also prove to be beneficial.
4. **The move towards open banking must be embraced.** Enhanced security must be **harmonised with digitization** efforts. An essential measure within this sphere is that of **collaboration with fintech.** An over-protectionist regime will simply hamper India's digitization efforts.

The Dialogue is a public-policy Tink-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues.

The Dialogue was ranked amongst the Top-Ten think-tanks in the world to watch out for by the Think-Tank Civil Societies Programme, Lauder Institute, University of Pennsylvania, in their 2020 and 2021 ranking index.

Email: info@thedialogue.co
Website: www.thedialogue.co

The Dialogue™
INFORM ENGAGE IDEATE